Blue Coat

Solution Brief: Blue Coat and Kaspersky

KASPERSKY lab

To protect information and maintain productivity, enterprises require a Web security infrastructure that can prevent all kinds of threats. Threats should never reach the desktop or other trusted asset. Blue Coat together with Kaspersky, provide layered defenses including a community watch cloud service and Web content controls combined with inline threat detection for all Web and secured Web (HTTPs) traffic.

Challenges

Since mid-2007 malware has exploded on the Web making it the number one threat vector, surpassing email which has held that position for years. In 2008 and 2009, around 15M new malware samples were uncovered in the Web each year – i.e., around 40 000 new malicious programs every day. Approximately 18,000 new URLs appear on the Web every day as part of the Web-based malware ecosystem.

2009 also saw a paradigm shift in malware lifecycles. Instead of wildfire-like outbreaks of relatively easily-contained viruses and worms, cybercriminals now create custom-tailored targeted malware with advanced functionality (such as rootkits) that proliferate through non-traditional channels such as social networks and P2P networks. This threat vector must now be secured as well.

Enterprises are facing the challenges of this evolving Web Security environment. Current desktop and email AV products play a vital role in a malware defense strategy. However, the growing abuse of the Web by cybercriminals, and the shift in focus witnessed in 2008-2009, requires additional measures to close this widening security gap. Enterprises need Web security solutions to prevent all threats hidden in HTTP and SSL encrypted traffic, file downloading, Web mail and Web 2.0 content.

Blue Coat Layered Defense

Blue Coat provides layered malware defenses to protect enterprises from all Web threats.

-> The first layer of defenses is Blue Coat WebFilter supported by real-time community watch cloud services – WebPulse™.

WebPulse analyzes over 1B user requests per week to support WebFilter's mission to proactively block hidden malware downloads in popular and trusted sites before they can penetrate the perimeter of the enterprise.

-> The second layer of defense is inline threat detection.

For attacks in live user sessions hidden behind user credentials, SSL encryption or obscured Web sites, community watch cloud services cannot proactively locate the malware before the user visits the site. So this defense requires inline threat analysis. Blue Coat has a strategic partnership with Kaspersky Lab to complete the inline threat analysis solution.

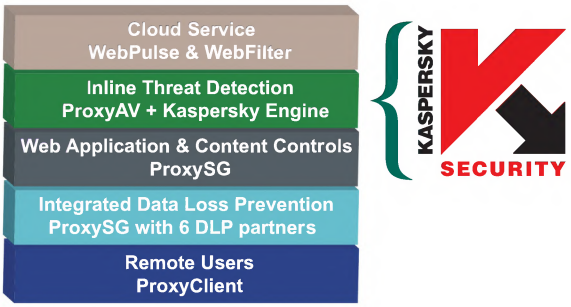
-> The third layer of Web application controls (e.g., IM & P2P) and Web content controls.

Suspicious (poor reputation) and unrated Websites should not be allowed to download files on to user desktops.

-> The fourth layer to control data leakage integrates with the third layer.

-> And finally, the fifth layer protects remote and mobile users.

The community watch cloud service provides an enhanced layer of protection over existing laptop defenses, plus central policy management and reporting when users are on networks you do not control.



Blue Coat and Kaspersky: Joint Solution

Inline threat detection with the Blue Coat ProxyAV™ appliance and the Kaspersky AV engine enables enterprises to prevent viruses, worms and Trojans from directly entering through open and hidden Web-based paths including:

-> Browser-based file downloads

-> Malware hidden in SSL traffic in order to to bypass existing virus scanning defenses

-> Personal Web email accounts where a majority of viruses, worms, and phishing scams propagate

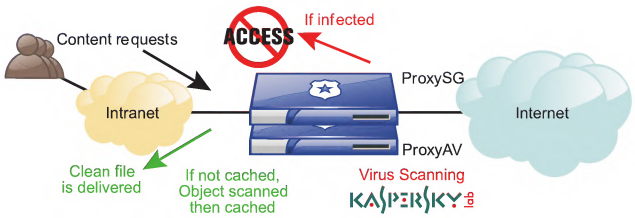
-> Web spam or email spam which may unknowingly activate Trojan downloads

Blue Coat and Kaspersky solutions combine to provide high performance and low latency AV scanning. ProxySG® content caching integrates with the ProxyAV and Kaspersky AV engine to further increase the performance of Web, secured Web (HTTPs) and file transfer protocol (FTP) virus scanning with a scan-once-serve-many solution. ProxySG intelligently maximizes bandwidth gains and improves the user experience. The ProxyAV provides additional performance gains by tracking checksum “fingerprints” of many non-cacheable objects, and avoiding unnecessary scanning if the identical object is downloaded again.

Blue Coat

Solution Brief: Blue Coat and Kaspersky

KASPERSKY lab



ProxySG runs on a purpose built, secure operating system specifically designed to provide fault tolerance, scalability and performance required for the largest Web AV installations. Latency remains flat with ProxySG and one or more ProxyAVs with Kaspersky AV engines allow the integrated system to scale performance. The ProxyAV is optimized for Web object anti-virus and anti-malware scanning and intelligently manages its resources, providing low latency scans for typical Web objects even when large downloads are scanned.

Features of Kaspersky AV for Blue Coat

Kaspersky Lab is a premier developer of advanced and highly effective anti-malware products, ensuring that the users of this joint solution get:

-> Comprehensive protection against all known kinds of internet threats

-> Frequent (at least hourly) updates of malware signature DBs, ensuring optimum update frequency-to-content ratio

-> Industry-leading zero-day protection (i.e., protection against malware that had only just appeared on the Internet), according to AV-Test laboratory tests

-> Very fast new threats response time – no more than 15 minutes in many cases

-> Largest number (> 4000) of packers and archivers supported

Furthermore, newer Blue Coat products incorporate the new version of Kaspersky Anti-Virus Engine, boasting the following new valuable features:

-> Faster scanning speed – 50% increase on Blue Coat Proxy AV 1400/2400

-> New signature databases: smaller DB size; better complex threats / rootkits detection; increased updates frequency

-> Lowest false positives rate

-> The joint solution keeps your malware inline detection at its best. These, in turn, combine with Blue Coat WebFilter on the ProxySG, for the ultimate Web gateway defense against today's multi-threaded malware attacks.

Joint Solution Benefits

The joint solution produced by Blue Coat and Kaspersky Lab is fully optimized and provides the following benefits:

-> Layered defenses against all threats – cloud service + inline threat detection + web application and content controls + integrated data loss prevention + remote user protection

-> A patent caching technology and special antivirus architecture has been developed for high performance and low latency virus scanning

-> Enhanced scanning performance and scalability in line with the requirements of large enterprises

-> World's fastest response to new malware threats to defend against zero-day attacks with minimum false positives

-> Maximum stability is guaranteed by Blue Coat scanning policy enforcement and is reinforced by Kaspersky best-in-class AV technology

-> The award-winning Blue Coat ProxySG / ProxyAV and Kaspersky Anti-Virus Engine provides proven benefits to protect information and maintain productivity

About Blue Coat

Blue Coat Systems is the technical leader in Application Delivery Networking. Blue Coat offers Application Delivery Network infrastructure to optimize and secure the flow of information to any user, on any network, anywhere which fuels a sustainable competitive advantage for distributed enterprises and organizations. Over 15,000 of the most demanding organizations, including 81% of the Fortune Global 500®, trust Blue Coat with their mission-critical applications. Additional information is available at www.bluecoat.com.

About Kaspersky Lab

Kaspersky Lab develops, produces and distributes information security solutions that protect customers from IT threats and allow enterprises to manage risk. Kaspersky Lab's products protect electronic information from viruses, spyware, adware, Trojans, hackers and spam for home users and corporate networks alike. Today, Kaspersky Lab's products protect more than 300 million users worldwide and its technology is licensed by leading security vendors around the world. Additional information is available at www.kaspersky.com.

Blue Coat Systems, Inc.
www.bluecoat.com

Corporate Headquarters
Sunnyvale, CA USA // +1.408.220.2200

EMEA Headquarters
Hampshire, UK // +44.1252.554600

APAC Headquarters
Hong Kong // +852.3476.1000